Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
	)	
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100
	)	

To: The Commission

COMMENTS OF
NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

7575 Colshire Drive
McLean, Virginia 22102
(703) 449-3993

April 8, 2011

Table of Contents

Executive Summary

As a leading provider of IT, systems engineering and systems integration, Northrop Grumman Information Services, Inc. ("Northrop Grumman") serves the Department of Defense, national intelligence, federal civilian and state and local agencies, and commercial customers. For more than 50 years, Northrop Grumman has assisted the public sector in building and operating IT systems that support critical missions that deliver services and protect citizens. While the selection of Long Term Evolution (LTE) as the air interface standard for the nationwide 700 MHz public safety broadband network is a good start toward true long-term interoperability, Northrop Grumman believes that unless the network build-out is properly overseen by responsible parties at a national level, the likelihood of a truly end-to-end interoperable network is small.

There are three critical issues related to the long-term success of this network that need proper attention:

- A National "Security and Identity Management" Strategy;
- A National "Common Network Applications" Platform; and
- A National "Certification, Validation, and Verification" Strategy.

Each of these issues is discussed in the following comments.

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Service Rules for the 698-746, 747-762 and 777-792 MHz Bands	)	WT Docket No. 06-150
	)	
	)	
Implementing a Nationwide, Broadband, Interoperable Public Safety Network in the 700 MHz Band	)	PS Docket No. 06-229
	)	
	)	
Amendment of Part 90 of the Commission's Rules	)	WP Docket No. 07-100
	)	

To: The Commission

COMMENTS OF
NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

Northrop Grumman Information Systems, Inc. ("Northrop Grumman")[1] hereby submits its Comments in response to the *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*[2] in the above-captioned proceeding, wherein the Commission proposes additional requirements to further promote and enable nationwide interoperability among public safety broadband networks operating in the 700 MHz band. Northrop Grumman supports the selection by the *Third Report and Order* of Long Term Evolution ("LTE") as a common technology

[1] Northrop Grumman Information Systems, Inc., a wholly-owned subsidiary of Northrop Grumman Corporation, is a leading provider of IT, systems engineering and systems integration for the Department of Defense, national intelligence, federal civilian and state and local agencies, and commercial customers. Northrop Grumman is a leader in public safety systems and one of the world's largest suppliers of 911 First Responder Computer-Aided Dispatch systems, as well as a major presence in homeland security initiatives as the number one provider of security solutions to the federal government. Northrop Grumman deploys next-generation secure broadband wireless networks and interoperable voice communications solutions for defense, intelligence, and public safety organizations, and has deployed the first large-scale secure mission-critical broadband wireless system for the public sector, covering the entire City of New York and serving a wide range of different public safety and government operations and entities.

[2] Third Report and Order and Fourth Further Order of Proposed Rulemaking, Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150 et al., released January 26, 2011.

platform for a Nationwide Public Safety Broadband Network,[3] and is pleased to comment on issues of interest to the Commission as requested. Northrop Grumman has concentrated our responses on particular areas of expertise where we believe there is an intersection of our corporate experience and specific areas of challenge to building the future national public safety network. In this document we will concentrate on responses related to "Public Safety Broadband (PSB) Wireless Network Security and Identity Management," "PSB Wireless Common Network Applications," and "PSB Network Certification, Verification, and Validation."

I. Introduction

Northrop Grumman Information Systems, Inc. is a wholly-owned subsidiary of Northrop Grumman Corporation. As a leading provider of IT, systems engineering and systems integration, we serve the Department of Defense, national intelligence, federal civilian and state and local agencies, and commercial customers. For more than 50 years, Northrop Grumman has assisted the public sector in building and operating IT systems that support critical missions that deliver services and protect citizens. Northrop Grumman provides unbiased engineering and vendor-neutral integration embracing best-of-class technologies and products which deploy and manage a wide range of networks.

Northrop Grumman is a leader in public safety communications systems; we are one of the world's largest suppliers of 9-1-1 First Responder Computer-Aided Dispatch systems. With a major presence in domestic security initiatives, we are the number one provider of security solutions to the federal government. Northrop Grumman has deployed next-generation secure broadband wireless networks and interoperable voice communications solutions for defense, intelligence, and public safety agencies across the world.

[3] Third Further Notice of Proposed Rulemaking, Service Rules for the 698-746, 747-762 and 777-792 MHz Bands, WT Docket No. 06-150 et al., 23 FCC Rcd 14301 (2008)("Third Further Notice"). A summary of the Third Further Notice was published in the Federal Register on October 3, 2008, 73 Fed. Reg. 57750.

By implementing wireless broadband networks that feature command-and-control software using video for integrated situation awareness and situation management, Northrop Grumman's work reflects how modern technology serves the government sector. These wireless networks provide high speed data, video and voice communications. More than 30,000 mobile data units are deployed to law enforcement and emergency response agencies nationwide.

Northrop Grumman's extensive experience as a systems integrator encompasses designing, building, and maintaining the systems public safety agencies will deploy in the Upper 700 MHz band. This experience emphatically shows that the number of technology options and providers has a direct relationship to innovation in system deployment and management, wider cost savings, and enhanced ability to respond to local or unique requirements. Northrop Grumman has participated in the 700 MHz band proceedings since their commencement, and supports the strategy to create an open standards solution for this network.

Northrop Grumman seeks to advise the Commission on some very key elements of implementing a Nationwide, Broadband, and Interoperable Public Safety Network in the 700 MHz band. While the selection of an air interface standard is a good start toward true long-term interoperability, Northrop Grumman believes that unless the build-out of the network is properly overseen by responsible parties at a national level the likelihood of a truly end-to-end interoperable network is small. When commercial carriers build networks they assure that, as it is built, each region provides the key technology, performance, and interconnect capabilities to the larger national network, even in situations where multiple vendor solutions may be part of the final implementation. Northrop Grumman has concentrated our responses on areas that we believe are "national level" challenges to the success of the eventual national public safety

network. Northrop Grumman believes there are three critical issues related to the long-term success of this network that need proper attention:

- A National "Security and Identity Management" Strategy
- A National "Common Network Applications" Platform
- A National "Certification, Validation, and Verification" Strategy

II. Public Safety Broadband Wireless Network Security and Identity Management

As a leading provider of security solutions to the US government and public safety agencies, Northrop Grumman is in complete agreement with the Commission's assertion that "secure communications are of vital importance to public safety and are needed to encourage increased usage and reliance on the network." While security is important for any communications network, it acquires a new meaning in the context of mission-critical public safety communication networks. The interests of the public safety community are best served by approaching the security requirements of the 700 MHz public safety broadband wireless networks in a holistic manner that addresses public safety's fundamental mission of protecting property and saving lives. As a case in point, public safety first responders depend on the 24x7 availability of their communications network to carry out their mission, inextricably linking reliability and security of the public safety networks. Weak and compromised network security undoubtedly reduces reliability and hence availability. Without the proper security measures in place no amount of reliability features, such as site hardening and backup power, can assure the highest degree of availability required of the public safety communications networks.

Northrop Grumman embraces the Commission's decision[4] to mandate the adoption of LTE as a technology standard for 700 MHz public safety broadband networks. Requiring a

[4] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 5, Adopted January 25, 2011; Released January 26, 2011.

common technology platform supports the critical goal of seamless interoperable communications across various 700 MHz public safety broadband networks as they get deployed in different states and local jurisdictions. Northrop Grumman also notes that LTE has become the technology of choice for the major commercial wireless carriers in the US and is poised to become the dominant global standard for broadband wireless networks. We contend, however, that the use of open and globally deployed standards, such as Internet Protocol (IP) that forms the core of the LTE-based public safety broadband wireless networks, considerably increases the vulnerability of these networks to malicious attacks, further underscoring the need for robust security mechanisms to protect these networks. The proof lies in the ever increasing number and sophistication of cyber attacks on ubiquitous IP-based technologies, including the Internet. Further, and equally significant, the requirements of commercial carriers to secure their wireless networks and user communications may not be as stringent as those of public safety. A security feature important to public safety and specified in the standard may never get implemented because the commercial carriers that drive the infrastructure market may not require that feature. In the event that the LTE standards or their implementation do not address the security and reliability requirements of public safety emergency communications, there will be a need to integrate additional capabilities and features so that the security requirements of public safety are fully met.

Northrop Grumman supports the Commission's tentative conclusion that three features for the network access security as specified in 3GPP TS 33.401[5] should be fully required. These

[5] 3rd Generation Partnership Project, "3GPP System Architecture Evolution (SAE); Security Architecture", 3GPP TS 33.401 (2008), available at http://ftp.3gpp.org/specs/html-info/33401.htm.

are also part of the requirements specified in the NPSTC BBTF[6] report. The three required network access security features are LTE signaling layer security over the Radio Resource Control (RRC) protocol layer, EPC signaling layer security over the Non Access Stratum (NAS) protocol layer, and user data/control layer security over the Packet Data Convergence Sub-layer (PDCP) protocol layer. Essentially, these three features together protect against attacks on the radio access link. Specifically, they provide mutual authentication of the user (actually the user device) and the network, as well as confidentiality of user data. Additionally they also protect the confidentiality and integrity of signaling data required to establish, maintain, and terminate the wireless communications link between the user and the network. However, it is important to note that these features protect user communication only on the air-interface link between the user device and the LTE base station (known as eNodeB). The protection terminates once the user information reaches the eNodeB. Also, the LTE standard does not protect the integrity of user communications, exposing it to security threats such as replay attacks.[7] Northrop Grumman recognizes the need to protect the air-interface given its inherent susceptibility to attacks and concurs with the Commission's conclusion that these features should be fully required. Northrop Grumman advises, however, that the radio access security features protecting the air-interface, though critical, do not provide the comprehensive end-to-end security required by the public safety practitioners to safely and securely execute their mission. Northrop Grumman recommends that other security features of LTE, besides the network access security, also be required. These security features include Network domain security, User domain security, Application domain security, and Visibility and Configurability of security. Northrop Grumman

[6] National Public Safety Telecommunications Council Broadband Task Force Report and Recommendations, September 2009.

[7] Replay attack is a term used in cyber security literature to describe attacks that involve intercepting sender data packets and replaying them back to the receiver at a later time in order to impersonate the sender.

recommends that the first three features be made a mandatory requirement. Each of these contributes to critical aspects of end-to-end security and, if not implemented, may expose the network and public safety users to disruptive and malicious cyber attacks. The last feature, Visibility and Configuration, informs the user whether a particular security feature is in operation or not and whether the use and provision of services should depend on the security feature. Although important, Northrop Grumman does not view this feature to be as critical as the other three. Even with these additional features, user information is protected only within the domain of the LTE network and not end-to-end from the user device to the public safety network operations and data center. As mentioned earlier, additional security solutions would need to be integrated with the LTE technology to enable end-to-end secure communications critical to public safety's mission.

Northrop Grumman also holds the view that, contrary to the common notion that security of communications networks only entails encryption to protect the privacy and integrity of the user information, it is actually much broader in scope particularly for emergency communications networks. While strong encryption is a critical requirement, equally important are the requirements for strong user and device authentication, protection for data residing on device, and physical security of the network assets such as communication towers, Network Operations Center and Security Operations Center. Although these requirements are outside the scope of the LTE specifications, they are critically important for public safety's mission and Northrop Grumman recommends that the Commission take an active role in promoting the standards for these requirements.

Northrop Grumman also thinks that it is entirely plausible for the nationwide public safety broadband wireless network to be shared by the federal government. During an emergency event, multiple agencies from all levels of government, including federal, state, and

local, will need to communicate and share information with each other in order to mount an effective and coordinated response. Northrop Grumman would like to note that the federal government follows its own standards and guidelines for exchanging and securing information as codified in the Federal Information Processing Standards (FIPS).[8] FIPS 140-2 is a NIST standard that specifies security requirements for cryptographic modules within a security system protecting sensitive but unclassified information. Because LTE's encryption schemes do not adhere to these standards in all cases, FIPS validated and certified solutions will need to be integrated with the public safety network in order to meet the government requirements for secure communications. In short, use of state-of-the-art technology for securing the network must be complemented with clearly defined and documented agency specific security policies and procedures, as well as personnel who are trained in implementing, monitoring, and enforcing these policies and procedures. An important aspect of security policy and procedures that cannot be overlooked is a well thought out contingency plan describing the sequence of actions that are needed to mitigate, limit, and contain damage in the unforeseen event that a security breach does indeed happen.

Although the topic of Roaming Authentication[9] is treated separately from Security in the FCC's *Third Report and Order and Fourth Further Notice of Proposed Rulemaking*, Northrop Grumman believes that the two are closely related to each other. An unauthenticated user on the network would be a serious and an unacceptable security breach. While the LTE standard includes a comprehensive framework for authentication, including roaming authentication, it

[8] Federal Information Processing Standards (FIPS) are standards and guidelines for information processing issued by National Institute of Standards and Technology (NIST) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

[9] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 21, 37, Adopted January 25, 2011; Released January 26, 2011.

applies only to the user device and provides mutual authentication between the user device and the LTE network. LTE's authentication mechanisms will have to be complemented by other robust authentication techniques such as multi-factor authentication to ensure that only authenticated and authorized users are able to gain access to the public safety network. With many public safety jurisdictions building their own private LTE networks, fail-safe mechanisms to authenticate users as they roam from their home networks to other jurisdictional networks become critical to maintain and sustain interoperability between different networks. Northrop Grumman recommends an approach that is consistent with the Commission's concept[10] of a clearing house function for efficient authentication of roaming users. The recommended approach is based on abstracting the geographically dispersed public safety networks into a single logical entity either as a "network of networks" or as a nationwide network that can be viewed as a single public safety enterprise. The authentication of all users, whether they are on their home geographical network or visiting other geographical network locations, should be handled by a single function that we call "Identity Management," which would reside inside a nationally managed and hosted Clearing House. This method is clearly scalable, as it does not require technical and administrative arrangements between individual jurisdictions to enable roaming or user movement throughout the system. It is also efficient and secure because it delegates the responsibility of managing the identity of all public safety users to one single entity. Identity Management could also incorporate different authentication rules for different jurisdictions depending on individual jurisdictions' needs. It could also provide different levels of authorization for access to resources and applications depending on whether the user is on their geographical home network or roaming throughout other network localities.

[10] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 21, 37 Adopted January 25, 2011; Released January 26, 2011.

Northrop Grumman believes that a key aspect of the overall success of the national network will reside in a comprehensive identity management scheme, backed by technology and standards. Network users should be identified on the network via common mechanisms used in industry (such as SIM cards), with extensions for further identification details. The details will include information such as credentials, role, access, and clearance levels. By using a common format nationwide users can be treated by the system across the entirety of the network as verified users, and the system can make decisions about security, Quality of Service, and access in a straightforward process. Each jurisdiction or agency will then be responsible to connect their existing enterprise to the LTE system using a clearly defined interface for identity and credentialing. Without this mechanism in place it is hard to see how a truly nationwide interoperable network can be created.

In summary, public safety communications networks are vital to the safety, security, and well being of the country and must be secured and safeguarded with the same heightened level of importance as any other critical infrastructure. As is well known, malicious attacks on our critical information and communication networks, also known as cyber attacks, have increased significantly in the past few years and they continue to grow in scope, complexity, and sophistication. The need for increased cyber vigilance has never been greater. Increasing network connectivity and interoperability improves information sharing and enhances situational awareness, but it also increases the vulnerability of these networks to externally mounted attacks. For example, a large scale denial of service attack on the public safety communications network during a crisis, just when it is needed the most, could have a crippling effect on the mission of our first responders. Many other types of attacks are possible, including injection of false information, corrupted key data, etc. The network needs to be strongly safeguarded and proactively monitored in an end-to-end fashion to avert casual as well as advanced persistent

threats. This should be accomplished by have a certified distributed protection strategy that is organized and managed on a national footprint by trusted experienced security engineering resources, just as other government agencies require such as DHS and the DOD.

III. Public Safety Broadband Wireless Common Network Applications

Northrop Grumman supports the Commission's tentative conclusion[11] that the five applications identified in the NPSTC BBTF report must be fully supported by each public safety broadband network. These five applications are (1) Internet access; (2) Virtual Private Network (VPN) access to any authorized site and to home networks; (3) a status or information "homepage"; (4) provision of network access for users under the Incident Command System; and (5) field-based server applications. A key objective of the public safety broadband wireless network is to achieve nationwide interoperability by creating an interoperable system of "network of networks" from the multitude of regional and tribal networks that would enable public safety users to communicate with each other and gain access to vital information and services regardless of their current location on the network. This goal can only be realized by considering interoperability at all communication layers of the network, namely the physical layer, the network layer, and the application layer. By mandating LTE and the associated Evolved Packet Core as a common air-interface standard and network platform for the public safety broadband wireless network,[12] the Commission has established a clearly defined framework for achieving physical and network layer interoperability. Application Layer interoperability, however, is a complex task with many other components of network design and operations such as security, priority, Quality of Service (QoS), and role-based access to services

[11] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 55 Adopted January 25, 2011; Released January 26, 2011.

[12] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 5 Adopted January 25, 2011; Released January 26, 2011.

and applications. Governance and policy issues are also required to distinguish between local network and roaming users in the provisioning of services and priority of access. Because users may not have access to all their applications or services on a visited network, integration of technologies such as mobile Virtual Private Networks with the public safety network may also be required to gain secure and authorized access to applications and services from a remote home enterprise. Northrop Grumman agrees with the Commission that requiring all regional and tribal networks to support the five applications listed above is an important first step in realizing the vision of application interoperability. These five applications together provide a common set of basic and essential data and information services to the public safety community on all public safety networks. However, it is feasible that this list is not the entirety of what applications may make sense for national implementation, and that other applications may lend themselves to providing national services(for example, location based services). In the following sections, we provide our comments with respect to some key identified applications.

Internet Access

One of the fundamental applications in the list is Internet access. In the context of Internet access, Northrop Grumman would like to draw a clear distinction between *private* IP-enabled networks such as the national public safety broadband network and *public* IP networks such as the Internet. The national public safety broadband network would be a dedicated private network designed to meet the highest standards of security, reliability, and availability required for emergency operations. Public safety agencies and jurisdictions throughout the nation will connect to this interoperable private network enabling fast, reliable, and secure access to mission critical data and applications. While the benefits of Internet access are numerous, Northrop Grumman contends that opening the mission critical national public safety network to the public Internet exposes it to a multitude of cyber attacks from our enemies and detractors around the

world due to the global reach of the Internet. Strong cyber-security measures would need to be put in place to protect the national network from cyber attacks mounted from the Internet. In light of these threats, Northrop Grumman emphasizes that access to the Internet from the national public safety network should be tightly controlled and proactively monitored to avert any unintentional or malicious threats. Northrop Grumman and other companies have designed, built, and operated internet access solutions for large scale government networks through providing security monitoring, incident management, patch and virus management, and remote user access solutions; it is our recommendation that internet access be controlled through a national gateway strategy and not left to individual jurisdictions. This approach will allow for a cost effective approach to protection and for forensics of cyber activity and events.

Remote Access VPN

By definition, Remote Access VPN provides secure access to an organization's network from remote locations over a public communications infrastructure such as the Internet. If one were to treat the national public safety broadband network as a single interoperable network with uniform policies for security and identity management across all tribal and regional networks, then the need for VPN may only arise if a user wishes to access the network from an external network such as the Internet. However, different jurisdictions are likely to have varying requirements for securing and protecting their information and data flow, which will require VPN access whenever users are outside of their local network and, in some cases, even when they are in their jurisdiction. Additionally, because the LTE network does not provide secure end-to-end access, VPN technology serves as a mechanism for addressing the end-to-end secure access requirements.

There are many different types of remote access VPN protocols, and one way of classifying them is by the Open Systems Interconnection (OSI) Layer they operate at. For

example, Layer-2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) are Data Link layer (Layer 2) VPN protocols, while IPSec, the most commonly used VPN protocol, operates at the network layer (Layer 3). Most VPN protocols work in a client server mode where a VPN client installed on a host device initiates a connection with the organization's VPN server. Authentication to verify user's credentials is performed at this stage. Data communication between the client and the host is typically encrypted and begins once the connection between the two is successfully established and authenticated. Clientless VPN solutions are currently available from the VPN software vendors that do not require installation of a client program on the user's device and are useful in instances where users may use a borrowed device or may not have rights to install software on their devices. Instead of using client software, these solutions create a Secure Socket Layer (SSL) VPN connection using the web browser on the user device. However, clientless VPN solutions from a number of companies have been found to be vulnerable to a variety of web-based attacks as reported in a November 2008 warning from the US Computer Emergency Readiness Team. Because of security weaknesses of the clientless VPN solutions, Northrop Grumman recommends against the use of clientless VPN solutions for security missions.

Remote access VPN protocols typically rely on tunneling methods to establish secure communications between the client and the VPN server in the organization's network. Essentially, tunneling is the process of encapsulating an entire packet within another packet and sending it over a network. Additionally, the encapsulated packets are protected from outside attacks by using encryption techniques. For example, L2TP is a tunneling protocol that encapsulates layer 2 Point-to-Point Protocol frames in IP datagrams and transmits them over a TCP/IP network connection. IPSec works similarly except that it encapsulates layer 3 IP packets

instead of layer 2 PPP frames. Because remote access VPN protocols such as L2TP, PPTP, and IPSec operate over the IP layer, they can easily be supported by the LTE network by virtue of it being an all-IP network. Northrop Grumman believes that because the LTE network is transparent to the commonly used VPN protocols, the choice of which VPN technology or protocol to use should be left to the individual jurisdictions. The VPN server could be hosted in the jurisdiction's network and data operations center without requiring any operational support from the LTE network infrastructure.

LMR Gateways

The value proposition of the broadband wireless network lies in an ecosystem of compelling, feature-rich applications tailored specifically for public safety and available to first responders, anywhere and anytime. Applications such as real time video streaming that enhance situational and operational awareness in the field provide substantial improvement to public safety operations and truly demonstrate the potential of the broadband network in direct contrast to the existing narrowband LMR networks. However, paramount and most essential to public safety is ensured mission-critical voice capability as provided by the existing LMR network. Northrop Grumman realizes that the standards for carrying voice on LTE networks are still evolving and it will several years before the technology becomes mature enough to be considered suitable for mission-critical voice communications. This implies that the current LMR networks and the public safety broadband networks will need to coexist and interwork to provide essential voice and data services to public safety for a considerable period of time. There are technologies in place and under development that provide interworking between LMR and broadband networks, including LMR gateways, which allow LMR radios and broadband devices to

communicate with each other. Northrop Grumman concurs with the BBTF recommendation[13] that LMR gateways should be supported by the public safety networks.

Northrop Grumman agrees with the Commission that an all-IP broadband wireless network will enable public safety to choose from a diverse array of applications and services to meet their communication needs. Northrop Grumman also supports the view that besides the five required applications as previously mentioned, individual jurisdictions should have the flexibility in choosing and deploying the applications that best serve their needs. Issues of interoperability may, however, arise if applications implementing a particular functionality are sourced from different vendors. A video streaming or finger print identification application from two different vendors may both run on the LTE network but may not be interoperable with each other due to differences in implementation, underlying operating systems, or client server interfaces. As a consequence, when responders from different jurisdictions or agencies converge on an incidence scene, some of them may not be able to use a critical application because its implementation on their device and their home network is different from the jurisdiction they are currently visiting. Northrop Grumman would request the Commission to take a note of this issue when requiring or mandating a set of applications for public safety. Northrop Grumman suggests that the national public safety organizations involved in the dialog with the FCC on issues related to the network may be able to help the commission to analyze the entirety of common applications necessary for proper national interoperability.

IV. Public Safety Broadband Network Certification, Verification and Validation Testing

Northrop Grumman endorses the Commission's recommendation[14] that adopting performance requirements for public safety broadband networks is necessary to ensure baseline

[13] 700 MHz Public Safety Broadband Task Force Report and Recommendations (2009) (*NPSTC BBTF Report)*

operability and efficient use of radio frequency resources, thereby paving the way for adequate network performance and interoperability. We also support the proposition of stipulating performance benchmarks for coverage and throughput performance at the cell edge. However, performance testing and measurement methodologies vary widely amongst different original equipment manufacturers (OEM) platforms, making it difficult to measure network performance against established performance standards for the public safety broadband networks. We recommend that the Commission address this concern by promoting a standard and uniform methodology for performance measurements to be used by all OEMs supporting the public safety broadband network implementation, and that system level testing validate the performance in field testing scenarios.

On the issue of conformance testing, Northrop Grumman concurs with the Commission on the need to have all public safety LTE User Equipment (UEs) pass the certification tests based on the 3GPP Release 8 standards for conformance (3GPP 36.141, etc.). Our experience with deploying and operating a wireless broadband network for mission-critical public safety communications has shown that there is need for network-wide verification and validation tests beyond those invoked within the FCC's *Third Report and Order and Fourth Further Notice*.[15] For example, vendor specific tests conducted within the PTCRB and GCF certification laboratories for interoperability of LTE network element interfaces provide validation only at a *"micro"* level, while the field testing on a live network captures performance benchmarks such as cell-edge throughput, coverage availability, handoff success rate, etc. and verifies "*macro*" level interoperability based on real-world networks performance. Both interoperability

[14] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 59 Adopted January 25, 2011; Released January 26, 2011

[15] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraphs# 106-110 Adopted January 25, 2011; Released January 26, 2011

components need to be tested using a unified approach and common performance criteria applied across all regions of the national public safety broadband network. There are several levels of testing that the LTE evolved packet system (EPS), comprising the radio access node (RAN), the evolved packet core (EPC) and user equipment (UE), must undergo to ensure compliance with the macro interoperability requirements. To this end, Northrop Grumman recommends establishing performance benchmarks and tests to measure against the performance benchmarks as part of the requirements for Public Safety Broadband Network interoperability. These tests may include the following:

- Field integration testing
- Performance testing – stress testing
- Reliability/Redundancy testing
- Security testing & certification
- System acceptance testing

As an example, key benchmarks may include items such as the following:

- 99.999% Availability for the backbone infrastructure – Verifiable
- 98% Coverage for Urban Areas – On-street Coverage translated to RF Signal Levels
- Certified Security – verified against both requirements and penetration testing

The work NIST is presently doing at the PSCR should be leveraged for identifying the certification, validation, and verification parameters for the overall network requirements.

Stress Testing

Beyond RF conformance testing, the LTE network must be tested for real-world operability in different user (morphology) environments and under different user traffic conditions. The public safety LTE broadband network must be dynamic and robust enough to

handle high user traffic surges associated with contingency periods during emergency incidents. Such incidences count on the resiliency and flexibility of public safety broadband network to support traffic surges far beyond the peaks typically experienced by commercial wireless carrier networks during busy traffic hours. A uniform process that simulates network stress conditions is therefore required to test the public safety broadband networks for successful operation during emergencies. The test processes and associated performance criteria should cover baseline (unloaded sites/network) as well as stress (loaded site/network) test conditions to ensure uniform network performance in critical times of need regardless of the vendor equipment and device types. Northrop Grumman advocates that the Evaluation and Testing Working (ETWG) group within NIST PSCR develop incidence based simulation processes and procedures as part of an overall performance framework for Public Safety Broadband Network.

Field Integration Tests

RF coverage verification and validation testing in the field is an important step in determining network operability for a given service availability requirement. This is often accomplished by detailed measurement campaign involving network drive tests designed to ensure environment-dependent and time-dependent signal variations are accounted for properly in the network site design. Coverage availability and reliability criteria under varying radio conditions and user traffic loads is first established then followed by a set of network quality tests to validate network performance against the set criteria. Parameters relating to network interference management should also be part of the mandatory testing requirements for network operability since the cell-edge throughput performance of the LTE network, critical during incidence operations, is affected by interference at the cell-edge.

Northrop Grumman agrees with the Commission's tentative conclusion[16] requiring the public safety broadband network to provide outdoor coverage at minimum single-user data rates of 256 Kbps (uplink) and 768 Kbps (downlink) for all device types at the seventy percent sector loading limits. These are practical limits allowing the system to linearly support increasing user demand from normal to incidence operations without dropping active public safety user traffic. However, based on our extensive experience with broadband network build and operations, we recommend that a reference bandwidth required for a given application (*e.g*. low-rate video) be defined in terms of its signal-to-noise ratio requirements and used to set bounds on the cell-edge requirements. Our recommended approach is borne from the need to address the variation of the cell-edge from the LTE cell site as the deployment environment changes from the dense urban area to a more open rural morphology.

In addition, it is important that the network procurement define clearly the boundaries of coverage required or desired by the local public safety stakeholders and that the test and verification of the performance be accomplished based on the defined geography of this required coverage area without compromise.

Security testing

Realizing that security is paramount to public safety communication, Northrop Grumman recommends a set of uniform processes and procedures to test and validate compliance with the public safety broadband network security requirements. As described in the Network Security and Identity Management section of our response, the security framework for public safety may need to integrate complementary technologies and solutions outside of the LTE standard specifications in order to meet the comprehensive end-to-end security requirements of public

[16] FCC Third Report and Order and Fourth Further Notice of Proposed Rulemaking, Paragraph# 61
Adopted January 25, 2011; Released January 26, 2011

safety. Extensive laboratory and field testing of these solutions will be required to ensure the safety and security of the public safety broadband networks without compromising the network performance. The Identity Management function proposed in this response by Northrop Grumman will also need to be tested to ensure compliance with the authentication requirements of the roaming public safety users. In light of increasing and continually evolving threats to the nation's critical infrastructure, Northrop Grumman also recommends that techniques for testing network resiliency continue to be developed and frequently refined to future-proof the network against such threats.

Northrop Grumman believes that ultimately it will be a necessity for a single national agency take responsibility for the "certification" of every portion of the national public safety broadband network for "secure operation." Because of the nature of the traffic and the national nature of the network operation, we believe that the "certifying authority" must have jurisdiction at a national level.

Application Inter Operability Testing

Testing for application performance requires that the performance benchmarks for user quality of experience (QoE) be established first. For example, video applications require benchmarks for video and audio quality, while latency is an important benchmark of quality for real time applications such as voice and location based services. Northrop Grumman recommends that the Commission include these benchmarks in establishing long term performance requirements for the network. Once the performance benchmarks are established, tests can be devised to measure the performance of applications against the set benchmarks. This will ensure an enhanced and optimal user experience in support of public safety's mission. This is no different from the processes commercial carriers use to assure the networks they build will run the applications they want to deliver to their customers.

Public safety responders need seamless access to at least the five application types listed in the Applications Section of this document during their everyday operations regardless of their location on the network. Tests will need to be performed in the field to ensure that first responders can access these applications from their home networks as well as when moving throughout other geography in the network. In an environment of multi-vendor devices with different operating systems, there is also a need to test for applications operability including performance across all device types supported on the public safety network. This will ensure that the public safety network delivers uniform user experience of applications across all devices.

V. Conclusion

Northrop Grumman urges the Commission to assure that in the areas of security, identity management, national level applications, and system certification, verification, and validation there is a sufficient national plan and practical strategy to assure the network's long-term success. Northrop Grumman believes that this will translate into the Federal Government working in cooperation with the Public Safety Spectrum Trust (PSST) and the other key national Public Safety organizations to assure that a national clearinghouse, national secure operations center, a national network certification, and a common national applications platform exists for purposes of operating a national public safety network.

Respectfully submitted,

NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

/s/ Robert F. Brammer, Ph.D.
Robert F. Brammer, Ph.D.
Vice President and Chief Technology Officer

/s/ Mark S. Adams
Mark S. Adams
Chief Architect Networks and Communications
Office of the CTO
ms.adams@ngc.com
571-313-2611

Northrop Grumman Information Systems, Inc
7575 Colshire Drive
McLean, Virginia 22102
(703) 449-3993

April 8, 2011